[10191/2007]

## UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|---|---|---|
| Applicant(s) | : | Andreas WESTENDORF et al. |
| Serial No. | : | 09/944,915 |
| Filing Date | : | August 31, 2001 |
| For | : | DATA TRANSMISSION METHOD |
| Group Art Unit | : | 2137 |
| Examiner | : | Michael J. PYZOCHA |
| Confirmation No. | : | 3903 |

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:
Mail Stop____AMENDMENT____
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on

Date:____3/13/2007____

Signature:_____
AARON C. DEDITCH
(33,865)

## TRANSMITTAL

SIR:

Transmitted herewith for filing in the above-identified patent application is an Amendment to a non-final Office Action, and another copy of a CERTIFIED English translation of priority German application DE 100043499.1-31.

While no fee is believed to be due, the Commissioner is authorized to charge any fees (including any extension fees) or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this transmittal letter is enclosed for that purpose.
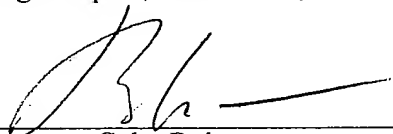
Respectfully submitted,

Dated: 3/13/2007

By:_____
Gerard A. Messina
(Reg. No. 35,952)
KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200

**CUSTOMER NO. 26646**

1207674

**Affidavit of Accuracy**

I, Gabe Bokor, of Accurapid Translation Services, Inc., hereby certify that the attached translation from German to English of a Patent Application entitled VERFAHREN ZUR DATENÜBERTRAGUNG [DATA TRANSMISSION METHOD] was performed by Accurapid Translation Services, Inc. on October 17, 2001. I also certify that our editor, who is a competent translator in the German and English languages, carefully compared the translation to the original, and that, to the best of my knowledge and belief, it is an accurate and full translation of the original text.

Poughkeepsie, October 17, 2001

Gabe Bokor

# DATA TRANSMISSION METHOD

## Background Information

The present invention relates to a data transmission method according to the definition of the species of the main claim.

5 A data transmission method is already known from German Patent Application 44 42 357 A1, where data is transmitted between a data processing device and a terminal. Before receiving the data transmission, there is a mutual authentification using codes stored in a security module in the data processing

10 device and in the terminal. Furthermore, a code is also transmitted, indicating whether the data records have been altered during the transmission. The security of the transmission is thus linked to the use of these security modules.

15

## Advantages of the Invention

However, the method according to the present invention having the features of the main claim has the advantage that data

20 transmitted to a first processor is also checked by transmission of second data based on the first data to a second processor and the correctness of the first data is checked by checking the second data. According to the related art cited, the security of a data transmission is guaranteed

25 only by the security module assigned to the terminal, but an additional check by an independent second processor is possible by the method according to the present invention. In particular, an unauthorized transmission of first data to the first processor can be determined by the second processor in

30 this way even if, for example, the first data originates from an unauthorized source, e.g., an unauthorized copy of a data

medium, or if, for example, first data is transmitted from a third processor by an unauthorized party. Data security is then no longer linked to a security module which could itself be stolen, but instead is guaranteed by the additional second

5    processor.

Advantageous refinements of and improvements on the method characterized in the main claim are possible through the measures characterized in the subordinate claims. It is

10    especially advantageous that error-free transmission of data is checked in the first processor and/or in the second processor, because this makes it possible to detect not only intervention in the data transmission but also transmission errors, and a transmission can be repeated after such a

15    transmission error has been detected.

It is also advantageous that the first data is transmitted to the first processor from a data medium drive or a third processor, and the identity of the third processor or the data

20    medium is checked by the second processor, because it is possible in this way to detect unauthorized copies of a data medium or a transfer from a third processor which is not authorized for data transmission.

25    It is also advantageous for the data to be transmitted in encoded form, in particular being encoded with a private key of the respective transmitting processor and with a public key of the respective receiving processor which is to be transmitted, because secure identification of the respective

30    transmitting processor is also possible directly in this way, in addition to a secure data transfer. Identification may be made on the basis of an electronic signature, i.e., an unambiguous counterfeit-proof electronic identification of the sender in data form.

35

In addition, a wireless transmission is also advantageous, because this eliminates the need for a connection to a stationary communications network, thus permitting mobile use of the method.

It is also advantageous that to check the second data, the second processor accesses a database which includes, for example, all the third processors authorized for transmission, all the authorized data media and/or all the first processors authorized for storing the respective first data, so that a comprehensive verification is possible.

It is also advantageous that a payment process is initiated by the second processor as a function of the second data, thus permitting calculation by the second processor of the first data transmitted. This makes it possible to ensure that a user using a program in the form of first data with the first processor will pay a fee only in the case of actual transmission of this data to the first processor. This makes it possible to ensure that a user need not pay for data until actually using it, and not when just having control over the respective data, e.g., due to possession of a data medium containing this data. It is also possible in this way to authorize payment processes by way of the second processor, i.e., payment processes in the form of credit card payments or purchase orders for goods or services whose data records have been transmitted to the first processor.

It is also advantageous that use of the first data is allowed by the second processor, so that the first data can be used in the processor only after this license has been transmitted to the first processor, i.e., release of the data by the second processor, so that this prevents use of unauthorized copies of the first data or false first data in the first processor.

It is also advantageous that use of the first data by the first processor is stored by the second processor, so that a user profile can be compiled for the first data on the basis of the data stored by the second processor.

It is also advantageous that a check is restarted in the first processor if the check has not been run through completely. This prevents individual steps in the check from being skipped in the event of an intentional or unintentional interruption in the checking process, e.g., due to a power failure.

It is also advantageous that a program for checking and/or a check result is stored in a nonvolatile form in the second processor. First, this prevents a possible counterfeiting of the program for checking the first data or falsification of a check result . In addition, a check of the first data need not be performed again with each restart of the first processor in the event the check result is stored in a nonvolatile memory.

It is also advantageous that the first data in the first processor is deleted if no user license for the first data is transmitted by the second processor. This prevents unauthorized use of the first data in the first processor. This is advantageous in particular when use of the first data is limited in time, so that in the case of a regular verification of a user license if deletion of the user license is detected after expiration of a preselected period of time, the first data is automatically deleted by the first processor.

It is also advantageous for a warning to be delivered if the first data is not released, so that a user is informed that he cannot use the first data and that he may optionally need to seek another source for acquiring the first data.

It is also advantageous if the second data includes a check code with respect to the first data or the identity of the first processor.

5      It is also advantageous to design a controller in a motor vehicle in particular as a first processor to which data is transmitted from a third processor or from a data medium. In particular in the case of systems in a motor vehicle which are relevant for vehicle safety, this permits a check on the data
10     transmitted, so that the function of safety-relevant systems in the motor vehicle cannot be endangered by defective data or data transmitted in an unauthorized manner.

Drawing

15

Exemplary embodiments of the present invention are illustrated in the drawing and explained in greater detail in the following description. Figure 1 shows a first exemplary embodiment of a device for carrying out the method according
20     to the present invention; Figure 2 shows a second exemplary embodiment of a device according to the present invention for carrying out the method according to the present invention; Figure 3 shows a third exemplary embodiment of a device according to the present invention for carrying out the method
25     according to the present invention; and Figure 4 shows a flow chart according to the present invention.

Description of the Exemplary embodiment

30     The data transmission method according to the present invention can be used for a variety of applications, in particular for different types of data to be transmitted. The data may include, for example, program data, i.e., data for controlling a processor or a device or data containing
35     information, e.g., data on telephone numbers, addresses and

regional maps or road maps. Furthermore, the first data
transmitted may also include, for example, data for a payment
process, a purchase process or an accounting process.
Accordingly, the first processor may also be designed as a

5      processor which controls a program sequence on the basis of
the first data, such as a controller in a motor vehicle or an
electric household appliance or an electric apparatus for
industrial use. The first processor may also be designed as
part of a device preferably for controlled playback of the

10     first data transmitted. Furthermore, the first processor may
be integrated into a device for executing the payment process,
purchase process or accounting process.

The method according to the present invention is explained in

15     greater detail below on the basis of its use for a controller
in a motor vehicle, in which case first data in the form of
program data and/or information is transmitted to the first
processor, i.e., the controller. This method can readily also
be used in other vehicles such as aircraft, ships or railcars.

20

Figure 1 shows a controller 1 in a motor vehicle 20, which is
connected to an automotive system 2. Automotive system 2 may
be, for example, an engine control unit which controls a
combustion process in the automotive engine or the power

25     conversion of the automotive engine; a display device in the
motor vehicle for displaying information to be displayed or a
navigation device which outputs driving instructions to a user
of the vehicle. A first processor 3 is arranged in controller
1. Furthermore, controller 1 has a nonvolatile memory 5 which

30     is divided into at least a first area 6, a second area 7 and a
third area 17. Controller 1 is also connected to a first data
medium drive 4 for a data medium 8, which is also arranged in
motor vehicle 20. In a device for data medium processing 10,
data medium 8 is written with data from a third processor 11

35     in a second data medium drive 9. Controller 1 is also

connected to a test unit 14 by a first wireless connection 12. Test unit 14 has a second processor 15 and a database 16 and is connected to an accounting office 13.

5    Data of third processor 11 is written by the device for data medium processing 10 to data medium 8 via second data medium drive 9. Data medium 8 is preferably an optical and/or magnetic data medium. When using an optical data medium, mechanical production of the data medium in second data medium
10    drive 9 is also possible. The device for data medium processing 10 is arranged outside motor vehicle 20.

Data medium 8 is introduced into motor vehicle 20 by a user and is inserted into first data medium drive 4. Data stored on
15    data medium 8 is read by first data medium drive 4 and transferred to first processor 3. First processor 3 recognizes newly transmitted first data and starts a program stored in first area 6 of nonvolatile memory 5 for checking the first data transmitted from third processor 11 to a volatile memory
20    of first processor 3 via data medium 8. First processor 3 establishes a first wireless connection 12 with test unit 14 and thus establishes contact with test unit 14. Furthermore, first processor 3 determines the second data, which is based on the first data transmitted, according to the program stored
25    in first area 6. The second data here may contain an identity number of data medium 8 and/or a check sum, i.e., the sum or the cross-check sum of a preselected sequence of bytes of the first data, segments or some other coding of the first data. In another exemplary embodiment, at least partial transmission
30    of the first data as second data to test unit 14 is also possible. The second data transmitted by controller 1 via first wireless connection 12 is checked in test unit 14 on the basis of a comparison with data stored in database 16. For example, it is possible to check an identity number of data
35    medium 8 and/or an identity number of first processor 3 here.

This makes it possible to check, for example, whether the owner of first processor 3 is authorized to use data medium 8. Furthermore, it is possible to check whether the first data stored on data medium 8 can be used by first processor 3, and in particular whether data medium 8 contains an authorized copy of the first data or whether the first data is in fact suitable for use in second processor 15 or 27, or whether it is a false or outdated version of the first data, for example. If this is the case, a user license is transmitted to first processor 3 over first wireless connection 12. First processor 3 stores in second area 7 of nonvolatile memory 5 the fact that first processor 3 is allowed to use the first data. In a preferred exemplary embodiment, at least a portion of the first data is stored in third area 17 of nonvolatile memory 5. The first data can also be stored in motor vehicle 20 in a bulk storage device (not shown in the figure) such as a hard drive which is connected to controller 1. The first data can then be used by first processor 3, either with access to data medium 8, third area 17 and/or the bulk storage device to control automotive system 2, e.g., a gasoline injection system, an engine control unit or a display unit. In a preferred exemplary embodiment, the issuance of the user license is relayed to an accounting office 13 which charges the user of motor vehicle 20 with the cost of using the first data, e.g., by charging the user's credit card account. In a preferred exemplary embodiment, first wireless connection 12 is established over a secure connection by having the second data to be transmitted encoded by first processor 3 and decoded again by second processor 15. Likewise, this is also true of the reverse transmission of a user license from second processor 15 to first processor 3. For coding, a private key of first processor 3 or second processor 15 is used in particular, so that it is possible to identify the processor making the transmission, and counterfeiting of a user license is prevented.

In a preferred exemplary embodiment, nonvolatile memory 5 is designed as a semiconductor component which is fixedly installed in controller 1 so that the check can be bypassed only by replacing nonvolatile memory 5. The device for data medium processing 10 may be in the possession of the user of the vehicle, loading data by calling it up over a data network such as the Internet and bringing it onto data medium 8 by way of this device for data medium processing 10 and thereby into motor vehicle 20. Furthermore, the device for data medium processing 10 may also be operated by a manufacturer of controller 1 or another commercial supplier of data for motor vehicle 20 or for controller 1. Improper or prohibited use of data in controller 1 can be prevented with a check by check unit 14, which is preferably also operated by the manufacturer of motor vehicle 20 or of controller 1. If a user license is refused by check unit 14 or if no response from check unit 14 arrives at first processor 3, the first data stored in first processor 3 is deleted in motor vehicle 20. In a preferred exemplary embodiment, a usage inquiry is made repeatedly with check unit 14 after preselectable intervals so that a time restriction on use of the first data is possible and can be verified.

Figure 2 illustrates a second exemplary embodiment of a device for carrying out the method according to the present invention. Here and below, the same reference numbers also denote the same elements. Controller 1 can be connected via a second wireless connection 24 to a central service office 21 which has a third processor 22 and a data memory 23. First data stored in data memory 23 can be called up from first processor 3 by the central service office over second wireless connection 24. Third processor 22 thus transfers the first data stored in the data memory over second wireless connection 24 to first processor 3 of controller 1 on request by first processor 3. A data medium drive in motor vehicle 20 is not

necessary in this exemplary embodiment, but it may be used in addition.

First wireless connection 12 and second wireless connection 24 are preferably designed as mobile wireless connections (e.g., GSM, UMTS). Second wireless connection 24 is designed in particular as a wireless connection which permits a high data throughput to permit transmission of even large volumes of data, e.g., for map data for a navigation system or for program data for an engine control unit within an acceptable period of time for a user. Furthermore, it is also possible that central service office 21, controller 1 and check unit 14 are all connected to a data network such as the Internet and there is communication among the individual units over the data network. A wireless interface for first wireless connection 12 may also be used for the second wireless connection.

Figure 3 illustrates another exemplary embodiment in which check unit 14 is replaced by a diagnostic device 26 which is connected to motor vehicle 20 or to controller 1 by a plug connection 25. A second processor 27 is arranged in diagnostic device 26 and is used to check the second data transmitted from first processor 3 over plug connection 25 to second processor 27. As shown in Figure 3, the first data can be supplied to first processor 3 over second wireless connection 24. In an exemplary embodiment which is not shown in Figure 3, a supply of the first data to the third processor by way of a data medium 8 according to the exemplary embodiment of Figure 1 is also possible. Through the use of diagnostic device 26, it is also possible to check on the correctness of the first data stored in controller 1, e.g., in a workshop, without establishing a wireless connection. A check can be started by diagnostic device 26, for example. Inadmissible first data can be deleted from controller 1. In a preferred exemplary

embodiment, diagnostic device 26 can be connected by a third wireless connection 28 to a database 30 in a second central service office 29 by way of which an identity of the first processor or a license to use the first data by the first

5      processor can be checked. Second central service office 29 is preferably operated by the manufacturer of motor vehicle 20 or the manufacturer of controller 1.

Figure 4 shows a first exemplary embodiment of the sequence of

10     the method according to the present invention. This method can be used for transmitting first data to the first processor by way of a data medium 8 and also by way of transmitting first data from a central service office 21. In an initializing step 40, the method according to the present invention is started

15     by inserting data medium 8 into first data medium drive 4. In a subsequent loading step 41, the first data is transmitted from data medium 8 to first processor 3. Then the checking operation is initiated with a determination step 42.

20     If the data is transmitted from a central service office 21 to first processor 3, the process sequence begins with an inquiry step 43 with which first data is called up by central service office 21 from first processor 3 over second wireless connection 24. In an encoding step 44, the first data is

25     encoded by third processor 22 and/or signed electronically and transmitted in a subsequent transmission step 45 to first processor 3. In a subsequent decoding step 46, the encoded and/or electronically signed data thus transmitted is decoded by first processor 3. In a preferred exemplary embodiment, a

30     publicly accessible key of first processor 3 is used for encoding and/or electronically signing the data in third processor 22, so that the data can be decoded and/or the electronic signature can be checked only by first processor 3, the first processor having the respective private key for

35     decoding. Furthermore, a private key of third processor 22 is

used for encoding, so that an unambiguous identification of the data source is possible. The check process is started with determination step 42. If the check process is interrupted before it has run, e.g., by a power failure, the check process

5    must at least be started again, beginning with determination step 42, where it is ascertained that a transmission of first data to first processor 3 has been terminated, i.e. where it is ascertained that the first data is available on a data medium. With the start of the subsequent check sequence, a

10   code for the fact that a check process is running is stored preferably in nonvolatile memory 5, preferably in second area 7 where the check result is stored. If the power supply to the controller is interrupted, then with a renewed start of controller 1, it is ascertained that a checking process has

15   not been terminated and the checking process is restarted, beginning with determination step 42.

Determination step 42 is followed by a first check step 47 in which a check is performed to determine whether the data

20   transmitted to first processor 3 has been transmitted correctly. A correct transmission is the case, for example, when there is error-free decoding in the case when the data has been transmitted in encoded form. Furthermore, parity data may also be added to the first data and used to detect a

25   transmission error. If it is found that the data has not been transmitted correctly, then the process branches off to a second check step 48 in which a check is performed to determine whether the transmission of data to first processor 3 has already been repeatedly unsuccessful. A tolerance

30   threshold can be preselected here. For example, if data is read from a data medium 8, multiple attempts to read the data from the data medium, which might be slightly soiled or damaged, can be made with no problem. If data is transmitted over a wireless connection, multiple repeats cause high

35   transmission costs. Therefore, the number of attempts should

be limited, e.g., to three transmission attempts. If it is found in the second check step that an error-free transmission was repeatedly not possible, then the process branches off to a final step 49 in which the user receives a warning that transmission or use of the first data in controller 1 is not possible. However, if it is found in second check step 48 that at least one more attempt to transmit the data should be made, then the process branches back off to loading step 41 or to transmission step 45.

If it is found in first check step 47 that the first data has been transmitted without errors to the first processor, then the process branches off to a transmission and transfer step 50, where a check code, e.g., a check sum, a sequence of certain characters of the first data or other preselectable parts of the first data is determined from the first data. Preferably an identity, especially an identity number of first processor 3, data medium 8 and/or third processor 22 is added to the second data. In determination and transmission step 50, this data is preferably encoded and/or signed electronically and transmitted to check unit 14 or to diagnostic device 26. Encoding of the second data makes it difficult to simulate a check unit 14 or a diagnostic device 26 and thus bypass a checking process of the first data through unallowed counterfeiting of a check unit 14 or a diagnostic device 26. In a subsequent third check step 51, an error-free transmission of the second data from first processor 3 to second processor 15 according to the exemplary embodiment of Figures 1 and 2 or to second processor 27 according to the exemplary embodiment of Figure 3 is checked. If no error-free transmission is found, then the process branches off to a fourth check step 52 where a check is performed to determine whether an error-free transmission of the second data has failed repeatedly. If it is found that there have been repeated failed attempts at correct transmission of the second

data, the number of the maximum transmission subject to error also being preselectable, then the process branches off to a final step 53. In final step 53, second processor 15 or 27 transmits to first processor 3 the result that the second data

5      could not be transmitted without errors. This is output by the first processor, e.g., on a display or over a loudspeaker (not shown in the drawing). If contact with the second processor is not possible, this is also detected and output by first processor 3. The check process is thus interrupted and

10     optionally resumed again at a later time, starting from determination step 42. If it is found in fourth check step 52 that a renewed attempt at transmission of the second data is possible, then the process branches off back to determination and transmission step 50, and the second data is again

15     transmitted from first processor 3 to second processor 15 or 27.

If it is found in third check step 51 that the second data has been transmitted correctly, then the process branches off to

20     fifth check step 54, where the second data is checked by second processor 15 or 27 to determine whether the first data on which the second data is based can be used in first processor 3. In this case, a check is performed to determine, for example, whether the first data is admissible data for use

25     in first processor 3. Furthermore, a check can be performed to determine whether the first data stored on data medium 8 is a licensed copy of the first data or whether an identity number of data medium 8 has already been registered for use on another first processor 3, and thus this is unauthorized use

30     of data medium 8 as an original or as a copy. Therefore, in a fifth check step 54, database 16 or database 30 is polled. Furthermore, a personal identification number (PIN) or a transaction number (TAN) to be entered additionally by a user into the first processor may also be checked here.

35

If it is found in fifth check step 54 that the first data in
first processor 3 must not be used, then the process branches
off to a prohibition step 55, where a prohibition against use
of the first data is transmitted to the first processor by
second processor 15 or 27. Then the process branches off to a
final step 56, where the first data in first processor 3 and
thus in first controller 1 and motor vehicle 20 is deleted. If
it is found in fifth check step 54 that use of the first data
by first processor 3 is allowed, then the process branches off
to a sixth check step 57, where a check is performed to
determine whether payment is required for use of the first
data by first processor 3. If payment is required, then the
process branches off again to an accounting step 58, where a
predetermined amount is billed to the user of motor vehicle 20
by accounting office 13, e.g., by a charge to a credit card.
If it is found in sixth check step 57 that no accounting is
necessary, then the process branches off to a license step 59.
License step 59 is also reached from accounting step 58. In
license step 59, a license to use the first data by first
processor 3 is transmitted to first processor 3. In a
subsequent use step 60, the check process is terminated and a
positive check result for a license to use the first data in
first processor 3 and a conclusion of the check process are
stored in nonvolatile memory 5. The first data transmitted to
first processor 3, e.g., program data or information data, can
then be used by first processor 3 due to the fact that the
program described by the first data is executed or the
information contained in the first data is analyzed and/or
output by first processor 3. This use is either unlimited in
time or is possible for a predetermined period of time, which
is then also preferably stored in nonvolatile memory 5. After
the end of this predetermined period of time, a check
according to the present invention is again performed,
starting from determination step 42, so that either the first
data is erased from first processor 3 and thus also from

controller 1 or a new calculation is performed with accounting step 58 of the check process, thus resulting in a further release.

What is claimed is:

1. A data transmission method, first data being transmitted to a first processor,
wherein second data based on the first data is transmitted to a second processor,
the second data is checked in the second processor, and a check result is transmitted to the first processor.

2. The method according to Claim 1,
wherein the first data is transmitted to the first processor from a data medium drive or a third processor.

3. The method according to Claim 2,
wherein the identity of the third processor and/or the data carrier is checked in the second processor.

4. The method according to one of the preceding claims,
wherein an error-free transmission of data is checked in each the first processor and/or in the second processor.

5. The method according to one of the preceding claims,
wherein the first and/or second data is transmitted in encoded form and/or with an electronic signature.

6. The method according to Claim 5,
wherein the data is encoded with a private key of the respective processor and/or is provided with an electronic signature.

7. The method according to one of the preceding claims,
wherein the first processor is connected to the second processor and/or the second processor is connected to the third processor by a wireless connection.

8. The method according to one of the preceding claims, wherein a database is accessed in the second processor for checking the second data.

9. The method according to one of the preceding claims, wherein a payment process is initiated by the second processor as a function of the second data.

10. The method according to one of the preceding claims, wherein use of the first data in the first processor is allowed by the second processor.

11. The method according to one of the preceding claims, wherein use of the first data by the first processor is stored by the second processor.

12. The method according to one of the preceding claims, wherein a check is restarted in the first processor if the check has not been run through completely.

13. The method according to one of the preceding claims, wherein a program for checking the first data and/or a check result is stored in a nonvolatile form in the second processor.

14. The method according to one of the preceding claims, wherein the first data in the first processor is deleted if no user license for the first data is transmitted by the third processor.

15. The method according to one of the preceding claims, wherein a warning is delivered if the first data is not released.

16. The method according to one of the preceding claims,

wherein a first check code is determined from the first data, and

the second data is formed at least in part from the first check code.

17. The method according to one of the preceding claims, wherein a second check code is determined from data of the first processor, and

the second data is formed at least in part from the second check code.

18. A device for carrying out the method according to one of the preceding claims.

19. A controller in a motor vehicle for carrying out the method according to one of Claims 1 through 17,

wherein the first processor (3) is positioned in the controller (1).

20. A check processor for carrying out the method according to one of Claims 1 through 17,

wherein the second processor (15, 27) is positioned in the check processor (14, 26).

21. A central service office for carrying out the method according to one of Claims 1 through 17,

wherein the third processor (22) is positioned in the central service office (21).

Abstract

A data transmission method is described, where first data is transmitted to a first processor, then second data based on the first data is transmitted to a second processor, and a check result is transmitted back to the first processor. This permits an independent check of data transmitted to a first processor by a second processor, so that abuse or prohibited use of first data in the first processor can be prevented.
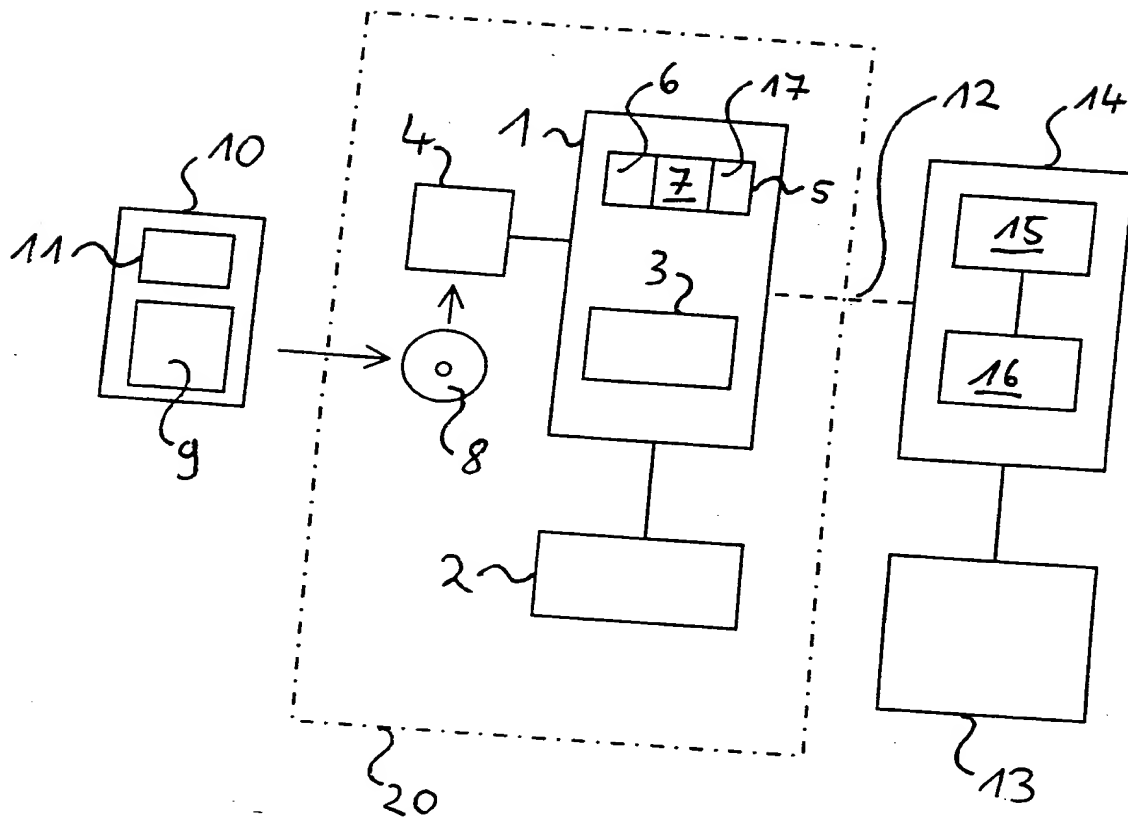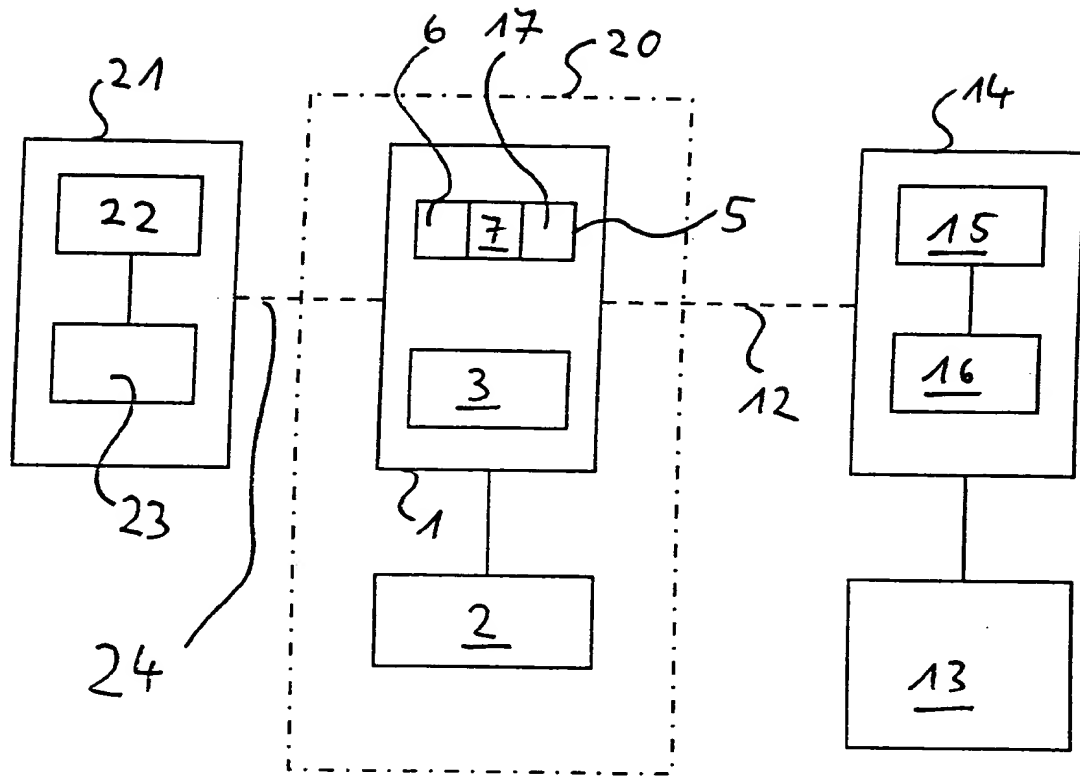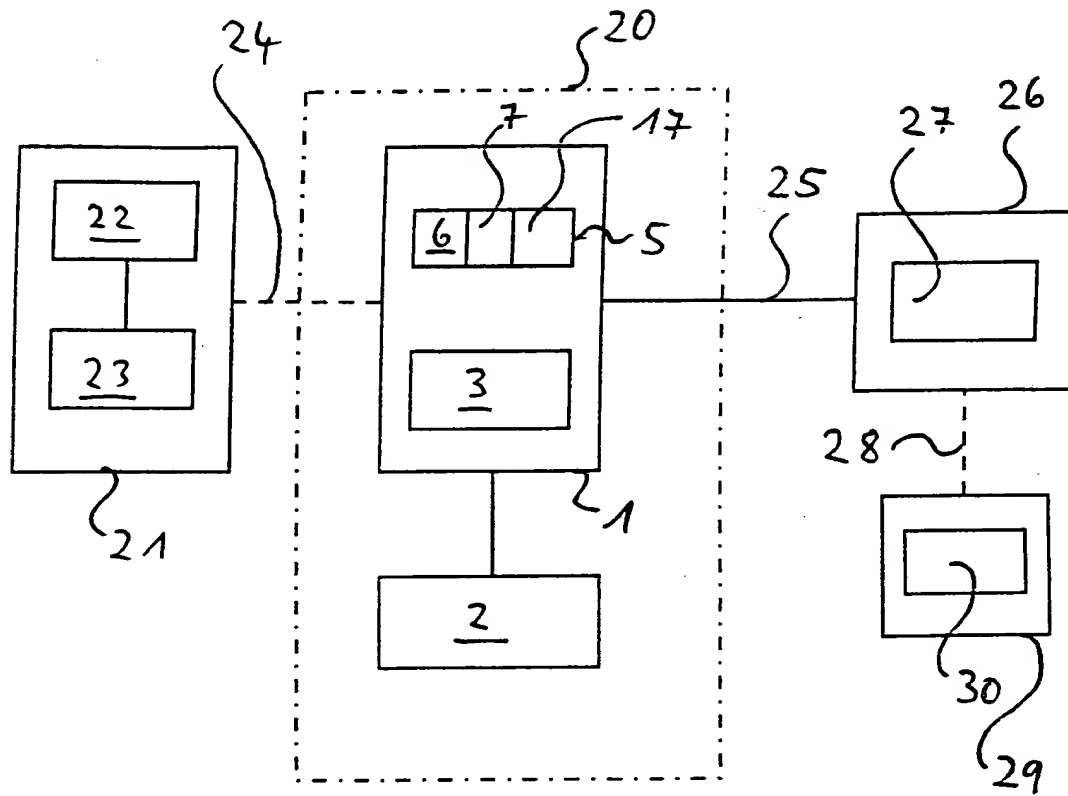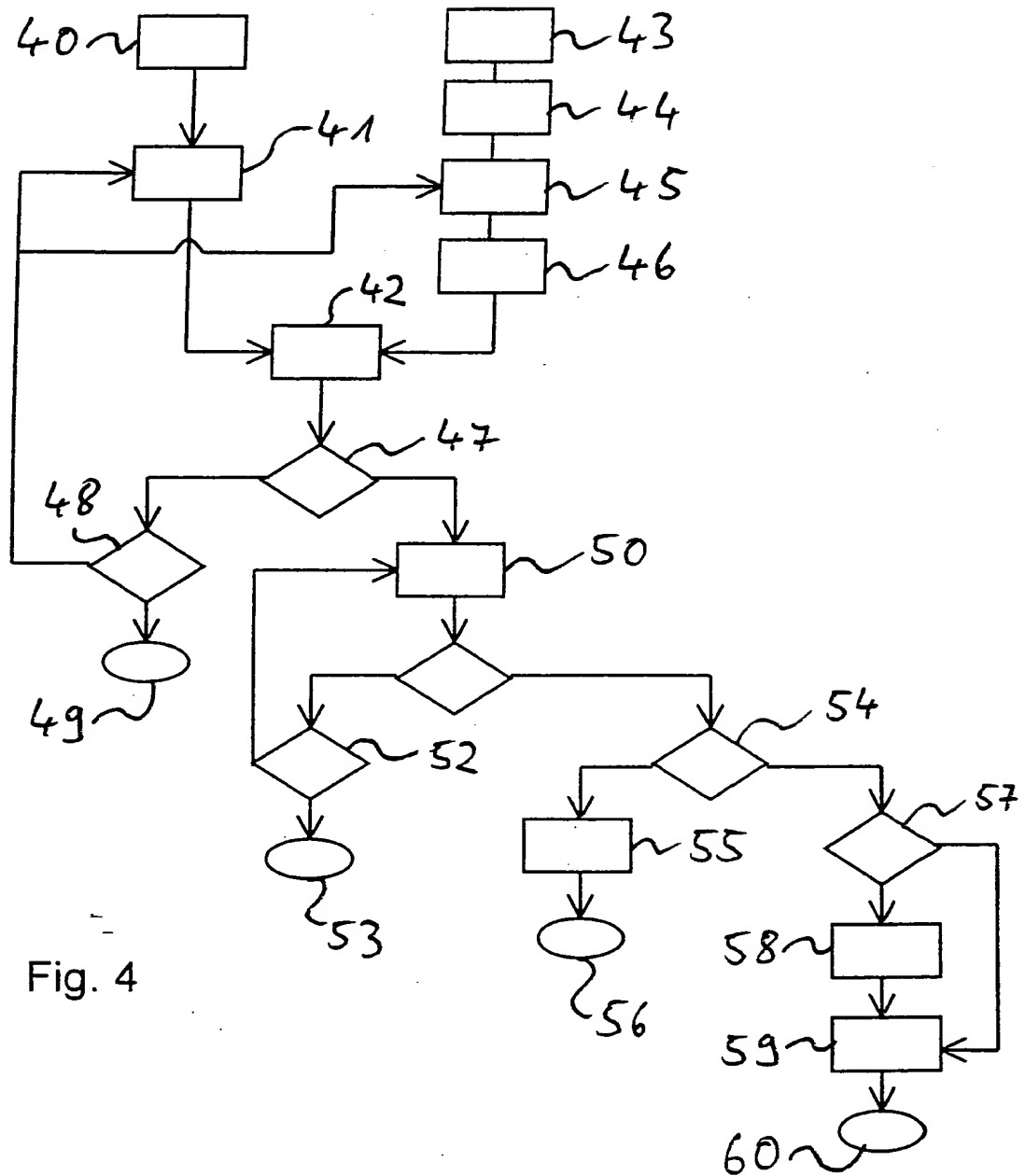
(Figure 1)

Fig. 1

Fig. 2

Fig. 3

Fig. 4